Department of Homeland Security
IAIP Directorate
Daily Open Source Infrastructure Report
for 07 September 2004

Current Nationwide Threat Level is
ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS
For info click here
www.whitehouse.gov/homeland

Daily Overview

- The Associated Press reports four terminals at Los Angeles International Airport were shut down early Saturday because of a security breach at one terminal and a separate incident at a security screening station in the Tom Bradley International Terminal. (See item 12)
- The Federal Emergency Management Agency has announced that 13 additional Florida counties are eligible for federal disaster aid to help meet the recovery needs of homeowners, renters and businesses battered by Hurricane Frances. (See item 25)
- The Philadelphia Inquirer reports that according to a new national study, the 20 largest school districts in the United States often are not doing enough to protect children in the event of an attack. (See item 26)
- IDG News Service reports that U.S. government agencies need to better understand the vulnerabilities of the software they're buying. (See item 34)

DHS/IAIP Update *Fast Jump*

Production Industries: Energy; Chemical Industry and Hazardous Materials; Defense Industrial Base
Service Industries: Banking and Finance; Transportation; Postal and Shipping
Sustenance and Health: Agriculture; Food; Water; Public Health
Federal and State: Government; Emergency Services
IT and Cyber: Information Technology and Telecommunications; Internet Alert Dashboard
Other: Commercial Facilities/Real Estate, Monument &Icons; General; DHS/IAIP Web Information

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://esisac.com]

1. *September 04, Associated Press* — **Nuclear transport ships head to U.S.** The first leg of a planned two−week shipment of weapons−grade plutonium to France from Charleston, SC, is underway. Two freighters loaded with naval guns and armed guards departed a British port for

Charleston on Friday, September 3, and will eventually pick up the material in the United States, according to a news release by Areva, a government−owned company in France coordinating the shipment. The freighters will transport the nuclear material to France, where it will be converted into fuel for a nuclear power plant. Officials want to test the material at the Catawba Nuclear Station on South Carolina's Lake Wylie. Areva said in a release it had "safely transported nuclear material over four million nautical miles without a single incident involving the release of radioactivity." **Federal officials have said the U.S. Department of Energy "has taken a hard look at sabotage and terrorism and determined that adequate safeguards remain in place to meet such threats in the post−September 11 environment." However, Tom Clements of Greenpeace International in Washington, DC, questioned the safety of launching the vessels during what already has proven to be a busy Atlantic hurricane season.**
Source: http://www.thestate.com/mld/thestate/news/local/9582503.htm

2. *September 04, The State Journal−Register (IL)* — **Police alert for cameras near plants. Springfield, IL, police took at least three reports in August of people seen snapping photographs or shooting video in the general direction of City Water, Light and Power's (CWLP) electric and water plants.** Since September 11, 2001, officials have become sensitive about people taking pictures of major pieces of infrastructure, apparently thinking it could be part of a plot to damage or destroy. Few pieces of infrastructure are more crucial in Springfield than the CWLP plant. The coal−fired generators there meet nearly all of the capital city's daily power needs, and the water treatment facility pumps out the 21 million gallons used on an average day. However, **officials say they don't believe last month's mini−rash of reports, called in by alert members of the public, indicates anything sinister is going on.** "In the past when people took pictures out there, nobody called in or thought a thing about it," said Ralph Caldwell, Springfield's assistant police chief and homeland security director. **"But since we started up homeland security ... and put it out there that we want people to pay attention, that has caused a few more people to call in."**
Source: http://www.sj−r.com/Sections/News/Stories/34392.asp

3. *September 03, News12.com (NY)* — **State grants Indian Point full authority on securing premises. Legislation in New York state has given full discretion to the security guards at the Indian Point nuclear power plants in Buchanan, NY, to protect the premises by any means necessary.** While federal law grants the plant to be self−enforced, officials of the plants' owner, Entergy, were unsure of whether the state granted legal authority for the plant to enforce the area as well. In addition to granting the plant's legal status, the state also earmarked money for a boat to be permanently stationed at the power plants, to help prevent people from entering the premises from the Hudson River.
Source: http://www.news12.com/WC/topstories/article?id=119164

[Return to top]

Chemical Industry and Hazardous Materials Sector

Nothing to report.
[Return to top]

Defense Industrial Base Sector

4. *September 03, Aerospace Daily & Defense Report* — **Single station to control multiple UAVs in demo. The U.S. Air Force later this year plans to show that it can control multiple unmanned aerial vehicles (UAV) from a single ground station, an ability that would help boost the contribution of such vehicles to network−centric operations,** according to Lt. Col. Eric Mathewson, chief of Air Combat Command's (ACC) UAV division. The multicontrol system will allow one pilot to fly four unmanned aerial vehicles at the same time. One beneficiary would be network−centric operations, which, he said, are being aggressively pushed by ACC. He said **UAVs alone will be significant contributors to this new kind of warfare because they carry sensors and "have the connectivity to disseminate what they're seeing at any given moment."** This means "you can task them directly to execute an ISR [Intelligence, Surveillance and Reconnaissance] mission." Or, in conjunction with a strike mission or a close air support mission, they're still gathering intelligence as they're transiting airspace. Instead of having downtime, you can actually access, once again, a sensor ... so when you talk about network−centric warfare, this would be the embodiment of certainly one aspect of it." Being able to control a number of UAVs from a single station would multiply the effect. Source: http://www.aviationnow.com/avnow/news/channel_aerospacedaily_story.jsp?id=news/uav09034.xml

5. *September 03, Government Accountability Office* — **GAO−04−973: Defense Acquisitions: Challenges Facing the DD(X) Destroyer Program (Report).** The DD(X) destroyer −− a surface ship intended to expand the Navy's littoral warfare capabilities −− depends on the development of a number of new technologies to meet its requirements. The Navy intends to authorize detailed design and construction of the first ship in March 2005. Government Accountability Office's (GAO) past work has shown that developing advanced systems that rely heavily on new technologies requires a disciplined, knowledge−based approach to ensure cost, schedule, and performance targets are met. Best practices show, for example, that a program should not be launched before critical technologies are sufficiently matured −− that is, the technology has been demonstrated in its intended environment −− and that a design should be stabilized by the critical design review. **Given the complexity of the DD(X) system and the number of new technologies involved, GAO was asked to describe the Navy's acquisition strategy for DD(X) and how it relates to best practices, and how efforts to mature critical technologies are proceeding.** GAO is not making recommendations in this report. Program officials agreed with our assessment of DD(X) program risks, but believe these risks can be mitigated. Highlights: http://www.gao.gov/highlights/d04973high.pdf
Source: http://www.gao.gov/new.items/d04973.pdf

[Return to top]

Banking and Finance Sector

6. *September 03, iTnews (Australia)* — **Users fooled by stolen ID scam. A new scam deceives users by falsely stating their identity has been stolen, directing the recipient to a trojan−unleashing Website, ACT (Australian Capital Territory) Policing warned recently.** "This latest e−mail scam is particularly shrewd as it appears under the title 'Your I.D. was

stolen' and then attempts to induce the recipient to visit a Website offering assistance," said Detective Sergeant Fiona Sagripanti. "If the Website is visited, a trojan is activated that allows the scammers to log the user's computer usage, which could include personal and financial details." Sagripanti warns phishing is on the increase and urges all users to exercise care. **"Not all virus protection programs will guard against users accessing Internet sites containing trojans," she said.**
Source: http://www.itnews.com.au/storycontent.asp?ID=3&Art_ID=21409

7. *September 03, Birmingham Business Journal (AL)* — **SouthTrust warns of scam. Birmingham, AL−based SouthTrust Corp. is warning customers to be wary of e−mails that claim to be from its security department. The e−mails, sent out en masse, may be an attempt to steal identities, according to the bank.** The messages, identifying the sender and subject lines as "SouthTrust Security," began circulating Friday, September, 3. The e−mail is seeking verification of Internet banking accounts and directs the recipient to a non−SouthTrust Website to fraudulently obtain the customer's account information. SouthTrust officials say they have no way of knowing how many e−mail messages were sent or how many customers may have received the e−mail. Bank employees are closely monitoring accounts for any unusual or potentially fraudulent activity.
Source: http://birmingham.bizjournals.com/birmingham/stories/2004/08 /30/daily29.html

8. *September 02, Associated Press* — **California schools warned of identity theft. California university officials have warned nearly 600,000 students and faculty that they might be exposed to identity theft following incidents where computer hard drives loaded with their private information were lost or hacked into.** Since January, at least 580,000 people who had personal information about them stored in university computers received warnings they might be at risk. **Over the year, problems have occurred at California State University, San Marcos, University of California −− San Diego and Los Angeles, and San Diego State University.** A California law requiring people be notified when they might be exposed to identity theft took effect in July 2003. Officials say that might explain the rash of notices. "There's no reason to assume that suddenly in July 2003 all these computer security breaches started occurring," said Joanne McNabb of the Office of Privacy Protection in the California Department of Consumer Affairs. "It's just that we know about them now, when we didn't hear before."
Source: http://www.washingtonpost.com/wp−dyn/articles/A57539−2004Sep 2.html

9. *September 01, Tribune−Review (PA)* — **Man accused of hacking, taking account numbers.** A Westmoreland County, PA, man was accused Tuesday, August 31, of being a computer hacker responsible for stealing more than 2,000 credit card numbers stored in the computer systems of businesses and corporations. Michael Ray Wally is charged with multiple counts of identity theft, unlawful use of computers, criminal use of a communication facility and attempted unlawful use of computers. **Wally is accused of posting the stolen credit card numbers on his Internet Website, HBX Networks, so that other people could use them to gain access to various Internet sites and other network components,** said Trooper Robert Erdely of the Area III State Police computer crimes task force. Some of the stolen numbers also were used to purchase goods and services, state police said. **Wally's Website bills itself as "a nonprofit organization with many goals," including documenting flaws and inadequacies of computer security systems and the ease with which they can be compromised. The**

Website details how Wally used a system called "war dialing" to access the computer networks of businesses and corporations. "War dialing" is basically the sequential dialing of various numbers until the right sequence comes up to gain access to a computer network.
Source: http://www.pittsburghlive.com/x/search/s_246645.html

[Return to top]

Transportation Sector

10. *September 04, Los Angeles Times* — **Cosmetics bag triggers airport alert in California airport. Hundreds of passengers were evacuated from a terminal at Ontario (CA) International Airport and dozens of flights were grounded Friday, September 3, when cosmetics in a carry−on bag activated an explosives−detection device, authorities said.** The airport's Terminal 4 was evacuated at 11:46 a.m. and a person held for questioning when security personnel found a suspicious bag, said Maria Fermin, an airport spokesperson. Flights were delayed until 2 p.m., when the Ontario Police Department's bomb squad determined that the bag contained only makeup. Neither Fermin nor police would explain why the makeup triggered the device, which is designed to detect traces of explosives.
Source: http://www.latimes.com/news/local/la−me−ontario4sep04,1,2553680.story?coll=la−headlines−california

11. *September 03, Transportation Security Administration* — **Secretary Ridge unveils Registered Traveler Pilot Program at Reagan National Airport .** In a continued effort to enhance aviation security and ease screening for thousands of travelers, the Department of Homeland Security's (DHS) Transportation Security Administration (TSA) on Friday, September 3, expanded operations for the Registered Traveler Pilot Program to Ronald Reagan Washington National Airport. American Airlines has been selected to partner with TSA at both Reagan National and Boston Logan airports. Similar pilots were launched successfully with other airline partners in Minneapolis (Northwest Airlines) and Los Angeles (United Airlines) in July and in Houston (Continental Airlines) and Boston in August. **"With the continuing success of pilot programs in Minneapolis, Los Angeles, Houston and Boston, TSA is demonstrating that the Registered Traveler Pilot Program can improve customer service and enhance our already strong layered system of aviation security," said DHS Secretary Tom Ridge. "This program also provides the Department with a national test bed for state−of−the−art biometric technologies that could provide far reaching benefits for many of the agencies that help to secure our homeland."** Each pilot program will last about 90 days at the five selected airports and is intended for frequent flyers on the partnering air carrier.
Source: http://www.tsa.gov/public/display?theme=44&content=090005198 00c9332

12. *September 03, Associated Press* — **Terminals at Los Angeles airport closed after security breach.** Four terminals at Los Angeles International Airport were shut down early Saturday, September 4, because of a security breach at one terminal and a separate incident at a security screening station in the Tom Bradley International Terminal, authorities said. The two incidents a half−hour apart on the busy Labor Day weekend appeared to be unrelated, said FBI spokesperson Cathy Viray. **The scare at the international terminal at around 8 a.m. apparently came when a flashlight battery exploded as it was being screened by a Transportation Security Administration (TSA) worker, Viray said.** The TSA worker

suffered minor injuries to his hands, Viray said. Airport spokesperson Tom Winfrey said the small explosion "slightly injured several people." The passenger whose bag was being screened at the time was begin questioned. **At 7:30 a.m., Terminals 6, 7 and 8 were evacuated after a passenger bypassed security at Terminal 8**, Winfrey said. Authorities cleared the terminals, which are connected, in order to re−screen passengers, he said.
Source: http://sfgate.com/cgi−bin/article.cgi?f=/news/archive/2004/09/04/state1353EDT0055.DTL

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

13. *September 03, Bozeman Chronicle (MT)* — **Park ponders bison vaccination. The National Park Service is beginning a formal study on the question of whether it should vaccinate bison for brucellosis, using "biobullets" fired from a pneumatic rifle. If it goes ahead, this will be the first vaccination of free−roaming bison in Yellowstone National Park.** The biobullets "are probably effective at a distance of about 100 feet," Yellowstone spokesperson Al Nash said. The biobullets would deliver the RB51 vaccine, which has been proven safe for use in the park. However, its effectiveness remains a matter of some debate. No vaccines are 100 percent effective for brucellosis. **The goal of vaccination program would be to "lower the percentage of Yellowstone bison infected with brucellosis," said a Park Service document posted on Yellowstone's Website.** About half of the park's herd of 4,000 or more bison has been exposed to the disease, which can cause an animal to abort its first calf after exposure. About 15 percent of the herd is actively infected. **Almost every winter, government officials kill bison that wander into Montana because of fears they will spread the disease to cattle.** Montana has been designated brucellosis−free since 1985.
Source: http://www.bozemandailychronicle.com/articles/2004/09/03/new s/vaccination.txt

14. *September 03, Dow Jones Newswires* — **Hurricane Frances has farmers scrambling. Farmers from Florida to New Jersey scrambled to harvest their fall crops Friday, September 3, ahead of Hurricane Frances.** "Many crops in the Southeast are ready for harvest and vulnerable to the strong winds and heavy rain that Frances will bring," said Farm Progress market analyst Arlan Suderman. Along with crop−damaging winds Frances was expected to produce a huge quantity of rain across the Southeast. The deluge comes at an especially bad time for Southeastern farmers, who recently began harvesting their 2004 fruit, vegetable, tobacco and grain crops. Less than half of all corn and only 19 percent of all soybeans in Georgia had been taken from the field entering this week, with harvest delayed by muddy conditions left behind by previous tropical storms and hurricanes. Wet conditions have also allowed mold and other fungal and/or bacterial diseases to affect some crops. In South Carolina, the cotton harvest has not yet begun. And just 47 percent of all corn had been collected, in addition to 18 percent of the state's grain sorghum and 25 percent of the 2004

apple crop.
Source: http://www.agprofessional.com/show_story.php?id=27200

15. *September 02, LaCrosse Tribune (WI)* — **CWD testing will continue. Minnesota and Wisconsin will continue chronic wasting disease (CWD) testing of wild white−tailed deer during fall hunting seasons, according to state wildlife officials. Both states will use a rapid screening test to detect possibly infected deer. Whitetails determined to be suspect with the rapid test will be re−tested using the immunohistochemistry test for CWD.** Minnesota is finishing its surveillance work of testing deer in all parts the state. The work began in 2002. Wisconsin completed its statewide surveillance testing last year. The only statewide testing this year will be of sick−appearing deer noticed by hunters and landowners. Testing will also continue in areas near captive deer populations that have tested positive for CWD. **Minnesota has not had any wild deer test positive for CWD, only two captive elk. Wisconsin has had 326 wild deer and some captive whitetails test positive for CWD since testing began in 2001.**
Source: http://www.lacrossetribune.com/articles/2004/09/02/outdoors/ 01second.txt

[Return to top]

Food Sector

16. *September 03, Dow Jones Newswires* — **Japan to meet on BSE issues. A panel of experts on Japan's Food Safety Commission is scheduled to meet Monday, September 6, to discuss Japan's bovine spongiform encephalopathy (BSE) safety measures including its cattle−testing requirement for the disease.** Masamichi Saigo, a communications official with the commission, said the panel could release an "interim" report after the Monday meeting, although it may cover only some of the BSE safety measures being discussed. **U.S. Department of Agriculture (USDA) Under Secretary J.B. Penn has said Japan's Food Safety Commission will play a major role in deciding if and how Japan will be able to lift its ban on U.S. beef.** Two key differences between U.S. and Japanese measures aimed at protecting consumers from BSE are on animal testing and requirements that bovine material deemed a risk of spreading the disease, called specified risk materials, be removed after slaughter. Japan continues to mandate that all cattle be tested for BSE, while the U.S. remains adamant that testing does nothing to ensure the safety of the human food supply, but is rather a means solely to judge the prevalence of BSE.
Source: http://www.agprofessional.com/show_story.php?id=27166

17. *September 02, Food and Drug Administration* — **Milk recalled. Spring House Creamery, of Michigan, announced Thursday, September 2, that their customers should return any Spring House Creamery Creamline Goat Milk carrying "sell−by" dates of 9/13, 9/15 and 9/17, and Creamline Cow Milk carrying a "sell−by" date of 9/6.** Please return recalled products to the store of purchase for a full refund. Recalled products should not be consumed. The recalled milk was distributed to parts of the Bay/Thumb and mid Michigan areas as well as throughout Southeast Michigan. Spring House Creamery assures their customers that this is a voluntary recall and no illnesses have been reported. **These products were not adequately processed to ensure pasteurization and may present a health risk.**
Source: http://www.fda.gov/oc/po/firmrecalls/creamline09_04.html

[Return to top]

Water Sector

18. *September 03, Water Tech Online* — **American Water announces major acquisitions. American Water, the largest private supplier of water services in North America, has completed water utility purchases through its Pennsylvania, Illinois, and Missouri subsidiaries, according to a company news release.** Pennsylvania American Water has purchased the water assets of Sligo Borough Authority for $430,000. As a result of the acquisition, Pennsylvania American Water will serve approximately 1,354 additional customers in the Sligo Borough and Piney Township, the company reported. In addition, Illinois American Water has acquired the Saunemin water system for $310,000. This water system currently serves 647 residents and will become part of the Illinois American Water system that currently provides water and/or wastewater services to more than one million people in 125 Illinois communities. Finally, Missouri American Water has acquired the assets of the Warren County Water and Sewer Company for $305,000 from a private company. The acquisition represents a significant commitment by Missouri American Water to 1,365 customers in Warren County. American Water operates in 29 US states, three Canadian provinces and Puerto Rico.
Source: http://www.watertechonline.com/news.asp?mode=4&N_ID=49978

[Return to top]

Public Health Sector

19. *September 06, U.S. Newswire* — **HHS deploys medical workers to assist Florida families.** Health and Human Services (HHS) Secretary Tommy G. Thompson announced Monday, September 6, that the department is coordinating the deployment of dozens of emergency medical personnel to provide assistance to communities damaged by Hurricane Frances. **HHS is deploying approximately 70 nurses and five pharmacists to four locations along the eastern seaboard of Florida to provide services to special needs shelters**. These shelters, located in Indian River County, St. Lucie County, and Martin County, are set up to provide basic nursing and medical care to individuals already suffering from sickness or injuries or at high risk of illness often due to age. **HHS also is assembling six additional teams to deploy to Florida, as the need arises**. The Secretary's Emergency Response Team is expected to deploy to Florida in the next few days to help survey and establish the overall short−term and long−term medical and health needs of the areas damaged by Hurricane Frances. In addition, **four Medical Reserve Corps (MRC) units are being used to increase medical staffing at shelters for people who evacuated their homes in the storm's path.** More information on personal safety in the wake of a hurricane is available at http://www.hhs.gov/news/facts/hurricane.html.
Source: http://releases.usnewswire.com/GetRelease.asp?id=35692

20. *September 05, Chicago Tribune (IL)* — **Databases aid war on bioterror. Powerful computer databases at the University of Chicago and the Argonne National Laboratory in Illinois are being enlisted in the war against deadly infectious diseases in an effort to safeguard**

against bioterrorism. University and laboratory officials announced Friday, August 3, the receipt of an $18 million grant from the National Institutes of Health (NIH) to create the National Microbial Pathogen Data Resource Center. The center will focus on eight pathogens, including bacteria that cause flesh−eating disease, cholera, toxic shock syndrome, anthrax and smallpox, said center co−director Rick Stevens, a University of Chicago professor and the director of the mathematics and computer science division at Argonne. With hundreds of research labs around the world pumping out new findings and advances almost daily, the center will collect and catalog the data and make it available to researchers through the Internet in hopes of speeding development of treatments for these diseases, Stevens said. **The project is among eight centers funded by the NIH in an initiative to boost the country's "bio−defense."**
Source: http://www.chicagotribune.com/news/local/chicago/chi−0409050048sep05,1,6719102.story?coll=chi−newslocalchicago−hed

21. *September 02, Newswise* — **Identifying tick genes could halt disease, bioterrorism threat.** Ticks can transmit a number of illnesses for which there is no vaccine and, in some cases, no cure. Ticks even could become bioterrorism weapons. To find new ways to control ticks and halt the spread of the pathogens they carry, Purdue University researchers and colleagues from the University of Connecticut Health Center, the University of Notre Dame, and Massachusetts Institute of Technology are undertaking the job of unraveling the genetic makeup of the deer or black−legged tick. **One of the potential outcomes of this project may be development of vaccines to block transmission of microbes that cause tick−borne illnesses.** Deer ticks are the main vectors for Lyme disease, which is the most commonly reported tick−transmitted human disease in the U.S. In 2002 the U.S. Centers for Disease Control and Prevention (CDC) recorded approximately 24,000 cases of the illness. This was a 40 percent increase over the previous year. **A number of ticks in the U.S. spread pathogens that the CDC considers potential bioterrorism weapons. The family to which I. scapularis belongs, Ixodidae, carries many of the microbes included on the CDC's Select Biological Agents and Toxins list.** Among the diseases caused worldwide by these organisms are Rocky Mountain spotted fever, tularemia, Crimean−Congo hemorrhagic fever, and tick−borne encephalitic diseases.
Source: http://www.newswise.com/articles/view/506900/

22. *September 02, Sun−Sentinel (FL)* — **Florida hospitals brace for Frances. Hospitals were preparing for Hurricane Frances on Thursday, August 2, attempting to keep the patients who must remain inside their walls safe, stockpiling supplies, and postponing elective surgeries and other procedures until South Florida returns to normal.** Many doctors' offices and health department clinics were closed, and pharmacies were rushing to fill extra orders as people tried to stock up on their medications in preparation for the storm. At least one hospital, Good Samaritan Medical Center in West Palm Beach, evacuated patients to two sister hospitals in the area. About 60 patients were moved to the safer locations, said Denise Rigopoulos, spokesperson for the hospital. She said **the decision was made after conferring with the county's emergency operations center.** Jupiter Medical Center administrators met Thursday to discuss a possible evacuation of patients but decided against it, said Stacey Brandt, hospital spokesperson.
Source: http://www.kansascity.com/mld/kansascity/news/nation/9567604 .htm?1c

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

23. *September 05, The Reporter (CA)* — **Radio communication top priority for Solano.** California's Solano County's Office of Emergency Services is working hard −− and spending a lot of money −− to make sure that countywide radio interoperability is coming soon, thanks in part to $3 million in federal homeland security funds. **Interoperability means Dixon, police can talk to Vallejo firefighters and sheriff's deputies in Rio Vista can talk to the Vacaville Police Department's dispatch center. "That was a major concern for us, that officials can't communicate with each other in a crisis,"** said Solano County Office of Emergency Services manager Bob Powell. "That was a huge problem on 9/11." Powell said the program is being made possible only by grants from Washington, DC. He said the interoperability project will use roughly $1 million of the $1.2 million in federal homeland security grants Solano County has secured this year.
Source: http://www.thereporter.com/Stories/0,1413,295~30195~2382733, 00.html

24. *September 05, Lawrence Journal−World (KS)* — **Kansas receiving millions to battle terror.** Chris Lesser can battle a brush blaze without clamoring into a heavy−duty fire suit, and he can look for people inside a burning house without opening a window, breaking down a door or chopping through a wall. Lesser's purchase of more than a dozen sets of lightweight personal protective gear and an infrared thermal imaging camera came courtesy of a $20,000 grant from the federal government. **The U.S. Department of Homeland Security oversees several programs pumping financial resources into local fire departments across the country. One program, known as the Fire Act, is poised to distribute 8,000 awards that will add up to $750 million.** "Through these funds, we will ensure that our nation's emergency responders have the equipment and training they need to respond to all hazards," said Tom Ridge, Secretary of the Department of Homeland Security. This year in Kansas, the program is pumping $3 million into new equipment and training for departments, many of them in rural areas.
Source: http://www.ljworld.com/section/stateregional/story/180512

25. *September 05, Federal Emergency Management Agency* — **Thirteen Florida Counties added for hurricane recovery aid.** The head the U.S. Department of Homeland Security's Federal Emergency Management Agency (FEMA) on Spetember 5 designated 13 additional Florida counties eligible for federal disaster aid to help meet the recovery needs of homeowners, renters and businesses battered by Hurricane Frances. **Michael D. Brown, Under Secretary of Homeland Security for Emergency Preparedness and Response, made the designations under the major disaster declaration issued for the state by President Bush.** The 13 counties added for assistance include Broward, Citrus, Glades, Hernando, Highlands, Lake, Miami−Dade, Okeechobee, Orange, Osceola, Pasco, Polk and Sumter. The counties initially designated for aid under the declaration were Brevard, Indian River, Martin, Palm Beach and

St. Lucie. **The assistance can include grants to help pay for temporary housing, home repairs and other serious disaster−related expenses not met by insurance or other aid programs. Low−interest loans from the U.S. Small Business Administration also will be available to cover residential and businesses losses not fully compensated by insurance.** Source: http://www.fema.gov/news/newsrelease.fema?id=13766

26. *September 04, Philadelphia Inquirer (PA)* — **Schools' readiness for crises criticized.** According to a new national study about to be released, the 20 largest school districts in the United States often are not doing enough to protect children in the event of an attack. Philadelphia is one of seven districts nationwide to be labeled "needs improvement" in a report by the nonprofit America Prepared Campaign, a New York−based group formed after the September 11, 2001, attacks. **Authors of the report, entitled "Preparedness in America's Schools," say Philadelphia's public schools need more emergency drills to prepare for possible attacks on the region's chemical and pharmaceutical plants and better information for parents on the district's emergency plans.** Dexter Green, director of security for the city's 185,000−student system, said the district had made major strides and is making the improvements highlighted in the report. He said that every district school already had an individual safety and crisis plan. The recent attack on the school in Beslan, Russia, reminded principals and teachers of the importance of emergency planning.
Source: http://www.philly.com/mld/inquirer/news/local/states/pennsylvania/cities_neighborhoods/philadelphia/9578175.htm?1c

[Return to top]

Information Technology and Telecommunications Sector

27. *September 03, SecurityTracker* — **Juniper Networks NetScreen−IDP may let remote SSH Servers overwrite files in certain cases.** A vulnerability exists in Juniper Networks NetScreen IDP that could allow a remote SSH server to overwrite arbitrary files on the target system in certain situations. This is due to an underlying directory traversal vulnerability in scp, the report said. This could lead to a remote SSH server being able to overwrite arbitrary files on the target system in certain situations. Original advisory and resolutions:
http://www.juniper.net/support/security/alerts/adv59739.txt
Source: http://www.securitytracker.com/alerts/2004/Sep/1011144.html

28. *September 02, Secunia* — **LHA multiple vulnerabilities.** Multiple vulnerabilities exist in LHA, which can be exploited by malicious people to compromise a user's system by executing arbitrary code and shell commands. The vulnerabilities have been reported in version 1.14 and prior. Original advisory and updates available at:
http://rhn.redhat.com/errata/RHSA−2004−323.html
Source: http://secunia.com/advisories/12435/

29. *September 02, SecurityTracker* — **OpenSSH default configuration may be unsafe when used with anonymous SSH services.** A configuration vulnerability exists in the default configuration of OpenSSH 3.9 and prior when used with anonymous public services such as anonymous CVS. **A remote user can connect to arbitrary hosts via the target service.**

Affected sites can place the following statement in their '/etc/ssh/sshd_config' configuration file to prevent attacks: AllowTcpForwarding no
Source: http://www.securitytracker.com/alerts/2004/Sep/1011143.html

30. *September 02, SecurityTracker* — **Opera 'embed' tag error lets remote users crash the browser.** A vulnerability exists in the Opera browser 7.23 build 3227 in the processing of the 'embed' tag. A remote user can create HTML that, when loaded by the target user, will cause the target user's browser to crash. Update to version 7.51: http://www.opera.com/
Source: http://www.securitytracker.com/alerts/2004/Sep/1011142.html

31. *September 02, SecurityTracker* — **HP Systems Insight Manager may not let users login after applying a Microsoft security patch.** The Microsoft security fix described in Microsoft security bulletin MS04−025 prevents users from logging in to HP Systems Insight Manager with Internet Explorer. This issue appears to be more of an incompatibility issue, rather than a security vulnerability. The vendor has issued a fix, available at: http://h18013.www1.hp.com/products/servers/management/hpsim/index.html?jumpid=go/hpsim
Source: http://www.securitytracker.com/alerts/2004/Sep/1011141.html

32. *September 02, SecurityTracker* — **Linux Kernel integer overflow in kNFSd lets remote users panic the system.** An integer overflow vulnerability exists in the Linux kernel in kNFSd. **A remote user can cause the target system to crash.** SuSE reported that there are various "signedness issues and integer overflows" in the kNFSd and the XDR decode functions in the Linux 2.6 kernel. A fix is available for the kNFSd overflow in the upstream 2.6.9−rc1 kernel version.
Source: http://www.securitytracker.com/alerts/2004/Sep/1011138.html

33. *September 02, Associated Press* — **Louisiana working on supercomputer network.** Technology experts are visiting Baton Rouge to look at ways for Louisiana to participate in the new National LambdaRail, an exclusive high−speed network of supercomputers around the country. The state Board of Regents now hopes to build a $25 million fiber−optics network linking super computer clusters among seven Louisiana universities that would join the LambdaRail node in Baton Rouge, which was designated as the Southeast region's access point between Houston, TX, and Jacksonville, FL. **Researchers for years have used Louisiana State University's supercomputer, called Super Mike, to model coastal erosion effects, for disaster management during hurricane season and to discover new findings in the petrochemical industry.** With an upgrade to Super Mike under way and access to the LambdaRail, state researchers will have unprecedented access to a virtual grid of the country's supercomputers −− allowing them immediate results to complex computing models.
Source: http://www.usatoday.com/tech/news/techpolicy/2004−09−02−la−l ambdarail_x.htm

34. *September 02, IDG News Service* — **U.S. government agencies aim for software assurance.** U.S. government agencies need to better understand the vulnerabilities of the software they're buying, said IT workers from several government agencies during a software assurance forum in Washington, D.C., last week. **The forum, sponsored by the Department of Defense (DoD) and the Department of Homeland Security (DHS), was the first step in a long−term discussion between government agencies and vendors on how to create more secure**

software, said Joe Jarzombek, deputy director for software assurance in the DoD Information Assurance Directorate. Prompting the forum was "a growing awareness of the fact that we've got a lot of vulnerabilties in the software we're acquiring," said Jarzombek. **A major concern among government IT workers is a need to understand how and where software is developed.** In many cases, software used by government agencies is developed by outsourced workers, Jarzombek said, and government purchasers need to know that information. Software developers should expect more security demands from customers in the near future, added Mike Rasmussen, principal analyst Forrester Research Inc. Government agencies are under pressure from Congress to improve their cybersecurity, and agencies are moving toward making more security demands of software vendors.
Source: http://www.infoworld.com/article/04/09/02/HNusgovt_1.html

35. *September 02, Associated Press* — **Microsoft warns spyware could bungle update. Microsoft is warning users of the Windows XP operating system to check for spyware before downloading the free massive security update, called Service Pack 2.** Barry Goff, a group product manager at Microsoft, said some spyware could cause computers to freeze up upon installation of the update. Spyware, which typically piggybacks with downloaded software such as file−sharing programs, tracks behavior, triggers pop−up ads and can otherwise cause problems on computers. **Microsoft recommends that users clean their PCs of spyware and back up their data before turning on the auto update feature that automatically downloads Service Pack 2 (SP2). People who download SP2 also may need to check whether legitimate programs, such as third−party security software, need to be updated.** Research firm IDC estimates that about 260 million copies of Windows XP have been sold.
Source: http://www.washingtonpost.com/wp−dyn/articles/A57501−2004Sep 2.html

36. *September 01, Computing (UK)* — **IT users seek to certify security.** IT security experts from some of the UK's most influential businesses are meeting this week to try to establish a professional body for certifying information security staff. **The group, which includes the Royal Bank of Scotland, Royal Mail and BP, will meet with The Information Security Forum, in an attempt to create an industry body which links financial and IT security needs.** David Lacey, Royal Mail director of information security, told Computing that the group hopes to establish codes of conduct and professional certification for IT security staff, to ensure compliance with growing corporate financial auditing regulations. Following the meeting, the group will expand its plans for security standards, benchmarking, business processes and vendor management. Lacey expects to produce a report before the end of October to share with IT suppliers.
Source: http://www.computing.co.uk/news/1157762

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: The US−CERT Operations Center strongly encourages Windows XP users to upgrade to Service Pack 2 if they have not already done so. SP2 offers significant protection against many of the emergent attacks that target Browser Helper Objects and Cross Domain Vulnerabilities in Internet Explorer. See http://www.us−cert.gov/cas/alerts/SA04−243A.html for more information.

Current Port Attacks

Top 10 Target Ports	1433 (ms−sql−s), 135 (epmap), 137 (netbios−ns), 1434 (ms−sql−m), 445 (microsoft−ds), 9898 (dabber), 5554 (sasser−ftp), 1026 (nterm), 1027 (icq), 3127 (mydoom) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

37. *September 04, Fort Collins Coloradoan (CO)* — **Scare empties Musgrave office. Congresswoman Marilyn Musgrave's Loveland, CO, office was evacuated for a few hours on Friday, August 3, during which it was the scene of a possible anthrax scare. A staff member opened a letter from which a white, powdery substance spilled. The building and its 75 to 80 employees were evacuated, including the office of Loveland Republican Senator Wayne Allard.** Within two hours, authorities gave the go−ahead to re−enter the offices, except Musgrave's campaign office, which remained the scene of an investigation. Preliminary tests showed the substance to be nontoxic. **It was the latest troubling incident for Musgrave. She has received "numerous" death threats during the past six to nine months.** Those threats have been relayed to the FBI. Congressional offices have been on alert for suspicious mail since shortly after September 11, 2001. U.S. Capitol mail has twice been shut down in the past three years because of letters laced with poisonous white powder. Source: http://www.coloradoan.com/news/stories/20040904/news/1176721 .html

[Return to top]

General Sector

38. *September 06, Bloomberg* — **Russia buries Beslan dead. Russia, on the first of two days of national mourning for the 335 killed in last week's Beslan school siege, buried the dead as the search continued for 260 people that are missing after the country's worst terrorist atrocity.** President Vladimir Putin, in an address to the nation on Saturday, September 4, promised to overhaul the country's corruption−ridden security forces to fight terrorism. The school raid was Russia's fourth terrorist attack related to Chechnya in the space of ten days. Two passenger planes crashed August 24 after explosions, killing 89 people, and ten died after a suicide bomb attack Monday near a Moscow subway station. More than 420 people, including

237 children, remain in hospitals, with 58 of them in a critical condition, state−run newswire Itar−Tass said Sunday. Terrorists held 1,181 people hostage in the school. **Released hostages and North Ossetian President Alexander Dzasokhov said the terrorists called for the withdrawal of Russian troops from Chechnya and the independence of the republic.** Troops launched their assault on Friday after bombs exploded in the school and **terrorists fired on hostages escaping the school's gymnasium**, said Valery Andreev, head of the North Ossetian division of the Federal Security Service.
Source: http://quote.bloomberg.com/apps/news?pid=10000087&sid=abxJS4stkwKg&refer=top_world_news

39. *September 06, Reuters* — **Frances leaves Florida in chaos.** Storm−weary Floridians emerged from hurricane shelters as Tropical Storm Frances moved off the state's west coast early Monday, September 6, after whipping off roofs, washing sailboats ashore and cutting power to nearly 6 million people. **Frances virtually shut down the fourth−largest U.S. state, home to 16 million people, for two days and promised damage not just to buildings but to the state's $53 billion tourism industry on the usually busy Labor Day holiday weekend.** Forecasters downgraded the storm, from which 2.5 million people had been urged to flee, from a hurricane to a tropical storm on Sunday, September 5, as it enveloped Tampa on Florida's west coast. Police and fire crews moved out into streets where Frances peeled away aluminum siding, tore boats from moorings, felled trees and shattered traffic signals. In Cocoa Beach, Frances shattered high−rise windows, stripped roofs off beachfront condos and tore apart at least two gas stations. Nearly 120,000 people were in public shelters, 3,400 patients were evacuated from hospitals and half a million sandbags were distributed to hold back floods, officials said. The hurricane hit hardest along a 150−mile stretch of Florida's east coast from Palm Beach to Titusville and the Space Coast, home to NASA's space shuttle fleet.
Source: http://www.reuters.co.uk/newsPackageArticle.jhtml?type=worldNews&storyID=577837&section=news

[Return to top]

DHS/IAIP Products &Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the IAIP Web page (http://www.nipc.gov), one can quickly access any of the following DHS/IAIP products:

DHS/IAIP Alerts − Advisories and Information Bulletins: DHS/IAIP produces two levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that addresses cyber and/or infrastructure dimensions with possibly significant impact.

DHS/IAIP Daily Open Source Infrastructure Reports − The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary and assessment of open−source published information concerning significant critical infrastructure issues.

DHS/IAIP Daily Reports Archive − Access past DHS/IAIP Daily Open Source Infrastructure Reports.

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 883−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 883−3644 for more information.

Contact DHS/IAIP

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

DHS/IAIP Disclaimer